ALMA MATER STUDIORUM · UNIVERSITÀ DI BOLOGNA

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea Triennale in Informatica

ANALISI E CRITICA DEL BORDER GATEWAY PROTOCOL

Tesi di Laurea in Materia Tesi

Relatore:
Chiar.mo Prof.
Fabio Panzieri

Presentata da:
Alessandro Santori

Seconda Sessione
Anno Accademico 2009/2010

Introduzione

In questa tesi verrà esaminato il protocollo di comunicazione **Border Gateway Protocol** (**BGP**)[1], che si occupa di instradare i pacchetti attraverso la rete Internet, la più grande "rete di reti" al mondo, per far comunicare fra loro reti *differenti*, aventi diversi schemi di indirizzamento, diversi protocolli di accesso al mezzo, diversi modelli di servizio e diverse politiche interne relative ad una singola rete. Quindi l'argomento maggiormente discusso è l'instradamento inter-dominio.

Lo scopo di questa tesi è quello di presentare le caratteristiche e le funzionalità del **BGP**, analizzarne ogni aspetto, valutare i pregi e i difetti, per poi successivamente trarre delle conclusioni in base all'analisi effettuata.

Dal momento che non esiste un'unica rete globale, ma esistono migliaia di reti in tutto il mondo, sorgono due importanti problemi nell'interconnettere tutte queste reti. L'*eterogeneità* e la *dimensione*.

Detto semplicemente il problema dell'eterogeneità consiste nel fatto che gli utenti di una rete di un certo tipo vogliono essere in grado di comunicare con gli utenti di reti di tipi diversi. L'obbiettivo dell'eterogeneità è quello di fornire un servizio utile tra host e ben prevedibile, usando questo groviglio di reti diverse. Il protocollo IP per ovviare a questo problema, definisce un modello si servizio di tipo best-effort che fa ipotesi davvero minimali sulle reti sottostanti.

Per comprendere il problema della dimensione della rete è utile considerare la crescita di Internet, che per venti anni ha pressappoco raddoppiato le proprie dimensioni ogni anno. Una crescita di questo tipo ci pone difronte a parecchie sfide.

Una di queste è l'*instradamento* (routing): come è possibile trovare un percorso efficiente attraverso una rete con milioni o, forse, miliardi di nodi? Un problema strettamente correlato a questo è l'*indirizzamento*, cioè il compito di fornire tanti indirizzi diversi per ogni nodo e calcolatore presente nella rete. Queste ultime due problematiche sono strettamente correlate tra loro sotto il punto di vista della *scalabilità*[3, 6].

Il problema della scalabilità degli indirizzi è stato risolto grazie all'indirizzamento gerarchico, con la suddivisione dell'indirizzo nelle sue parti, la parte che identifica la rete e quella che identifica l'host; questa tecnica ha migliorato la scalabilità di una rete di grandi dimensioni come è quella di Internet. In questo modo, i router, contengono tabelle d'inoltro che elencano soltanto numeri di rete, piuttosto che tutti i nodi della rete. Quello che interessa maggiormente questo lavoro è il problema della scalabilità dell'instradamento, cioè trovare il modo di minimizzare la quantità di numeri di rete che vengono fatti circolare dai protocolli di instradamento e memorizzati nelle tabelle di instradamento dei router. Vedremo come si possa usare la gerarchia per migliorare la scalabilità dell'instradamento, sia mediante l'instradamento inter-dominio, sia all'interno di un singolo dominio.

Prima di iniziare a parlare del BGP introdurremo, nel primo capitolo la definizione di Sistema Autonomo (**AS** Autonomous System), da cosa è formato, e soprattutto a quale scopo rispondono.

Nel secondo capitolo entreremo nel merito della questione, parlando dei problemi dell'instradamento inter-dominio, del funzionamento e delle caratteristiche del BGP.

Il terzo capitolo discuterà delle politiche di sicurezza e dell'affidabilità del protocollo, mostrando diversi meccanismi e confrontandoli fra loro.

Il quarto capitolo analizzerà alcuni aspetti fondamentali del BGP, quali la convergenza, la stabilità di routing e la topologia della rete.

Nel quinto e ultimo capitolo, infine, vengono fatte delle considerazioni conclusive sull'argomento.

Indice

Elenco delle figure

Capitolo 1

Autonomous System

1.1 Definizione

La classica definizione di Sistema Autonomo[4], è un insieme di router, host e reti, amministrati da una singola e ben definita entità amministrativa, che usano protocolli intra-dominio e metriche comuni per indirizzare i pacchetti all'interno del sistema autonomo, e usano protocolli inter-dominio per instradare pacchetti ad altri sistemi autonomi.

Un' entità amministrativa si contraddistingue sia in base ad elementi informatici, come ad esempio politiche di routing ben precise, sia per motivi appunto amministrativi. Un esempio di sistema autonomo può essere quello che contraddistingue gli utenti di un unico provider, oppure, più in piccolo, quello che costituisce la rete interna di un'azienda. In origine la definizione richiedeva il controllo di una singola entità, di solito un Internet service provider o un'organizzazione molto vasta con connessioni indipendenti a diverse reti, che aderisce ad un'unica e ben definita politica di routing. Con la crescita della rete, diverse organizzazione possono utilizzare diversi AS privati collegati ad un ISP che, a sua volta, li collega tutti ad Internet. Anche se ci sono diversi sistemi autonomi supportati dall'ISP, Internet visualizza solo la politica di routing dell'ISP, che deve avere un numero di sistema autonomo ufficialmente registrato (ASN). Questo numero è importante nel routing, perchè identifica in modo univoco ogni rete presente in Internet.

Dato che in Internet i sistemi autonomi vengo detti anche *domini*, chiameremo l'instradamento (routing) all'interno di un sistema autonomo come *instradamento intra-dominio*, mentre quello direzionato verso altri sistemi autonomi con il nome di *instradamento inter-dominio*[5].

Per definirlo in modo sintetico, un AS è un insieme di uno o più prefissi IP connessi da uno o più operatori di rete il quale hanno una singola e ben chiara politica di routind definita.

1.2 Perchè

Dal punto di vista dell'instradamento inter-dominio, l'Internet globale è vista come un'insieme di diversi AS (Autonomous System) arbitrariamente interconnessi fra loro. Il motivo di questa visione, risiede nel fatto che l'instradamento presenta un problema di scalabilità[6], cioè la capacità da parte di un sistema di crescere, o decrescere, in funzione delle necessità o delle disponibilità.

Se tutti le reti, gli host e i vari nodi non fossero aggregati in un sistema autonomo ci troveremmo in una situazione ingestibile, dato che i nodi dovrebbero memorizzare e scambiarsi una quantità elevata di informazioni, favorendo problemi prestazionali. Quindi una tecnica utilizzata per risolvere questo problema è l'aggregazione gerarchica, in questo caso in sistemi autonomi. Così facendo i nodi all'interno di un AS non dovranno preoccuparsi di mantenere informazioni riguardanti percorsi di nodi all'interno di altri AS, ma solo quelli appartenti al proprio AS. Per questo motivo bisogna minimizzare la quantità di numeri di rete che vengono fatti circolare dai protocolli di instradamento e memorizzati nelle tabelle interne dei router, in Internet, in modo da migliorarne le prestazioni, e non avere problemi di scalabilità.

L'uso del termine Autonomous System sottolinea anche il fatto che, anche quando vengono utilizzati diversi protocolli interni, la gestione di un AS, sembra agli altri AS, avere un unico piano di instradamento interno, coerente, e presenta un quadro logico delle reti che sono raggiungibili attraverso esso.

Oltre a migliorare la scalabilità, il modello di sistema autonomo disaccoppia l'instradamento intra-dominio che avviene in un AS da quello che avviene in un altro AS, in modo che ciascun AS possa eseguire il protocollo intra-dominio che preferisce: può addirittura usare percorsi statici, o perfino più protocolli di instradamento contemporaneamente. Il problema dell'instradamento inter-dominio si occupa, invece, di fare in modo che diversi AS condividano l'uno con l'altro le informazioni di raggiungibilità.

1.3 Tipi di AS

Gran parte del traffico di rete trasportato all'interno di un AS ha origine o termina in nodi che si trovano all'interno dell stesso AS, questo tipo di traffico si chiama "traffico locale". Il traffico che non rientra in questa descrizione si chiama "traffico di transito". In base a come un AS tratta il traffico di transito, lo si può classificare in tre modi diversi:

- AS di tipo *stub*: AS che ha una singola connessione verso un altro AS, e quindi trasporta solo traffico locale.
- AS di tipo *multihomed*: AS che ha connessioni con più AS, ma rifiuta di trasportare traffico di transito.
- AS di tipo *transit*: AS che ha connessioni con più AS ed è progettato, sotto certe restrizioni politiche, per trasportare sia traffico locale che traffico di transito.

Quindi all'interno di un sistema autonomo possiamo distinguere quattro tipi di router differenti, in base al traffico che devono inoltrare:

- Router interni (*I*nternal Router): sono quelli che si trovano completamente all'interno di un'area, diversa dalla backbone (dorsale Internet) ed eseguono solo l'instradamento intra-dominio.
- Router di bordo area (*B*order Router): questi router appartengono sia ad un'area, sia alla backbone, che collegano due o più aree.
- Router di dorsale (*B*ackbone Router): questi router eseguono l'instradamento entro la dorsale, ma non sono router di bordo area.
- Router di confine (*B*oundary Router): scambiano informazioni di instradamento con router appartenenti ad altri AS. Questo router può, per esempio, utilizzare il BGP per compiere l'instradamento interdominio. È attraverso questo tipo di router di confine che gli altri router apprendono i percorsi verso reti esterne.

Capitolo 2

Instradamento inter-dominio

2.1 Il problema dell'instradamento inter-dominio

Come detto in precedenza il problema affrontato in questa tesi riguarda l'instradamento inter-dominio[3]. Nonostante le discussioni sull'instradamento sono focalizzate generalmente sull'identificazione dei percorsi ottimali basati sulla minimizzazione di una qualche metrica delle linee di collegamento, il problema dell'instradamento inter-dominio si rileva talmente complesso che gli obiettivi sono più modesti: cioè trovare un percorso *qualsiasi* verso la destinazione finale, che sia privo di cicli. In sostanza, siamo più interessati alla raggiungibilità che all'ottimizzazione.

Esistono diversi motivi che rendono difficile l'instradamento inter-dominio. Prima di tutto, c'è il problema della dimensione. Un router di una rete backbone in Internet deve essere in grado di inoltrare pacchetti destinati a qualsiasi punto della rete, per cui deve avere una tabella di instradamento che fornisca una corrispondenza per qualsiasi indirizzo IP valido.

La seconda sfida viene dalla natura autonoma dei vari domini. Ciascun dominio può eseguire, al proprio interno, protocolli di instradamento diversi e usare qualsiasi schema, di propria scelta, per assegnare i costi ai percorsi. Ciò significa che è impossibile calcolare costi significativi per percorsi che attraversino più AS. Il risultato è che l'instradamento inter-dominio publicizza soltanto la "raggiungibilità", cioè, in sintesi, l'affermazione che "tramite questo AS si può raggiungere quella rete". Vuol dire anche che scegliere un percoso ottimale per l'instradamento inter-dominio è sostanzialmente impossibile.

La terza sfida è rappresentata dal problema della fiducia. Il fornitore di

servizi A potrebbe essere scettico nel credere ad alcune affermazioni publicizzate dal fornitore B, per timore che esso publicizzi informazioni di instradamento errate. Ad esempio, confidare nel fatto che il fornitore B publicizza un'eccellente percorso verso qualsiasi destinazione di Internet può essere una scelta disastrosa, nel momento in cui si scopre che il fornitore B ha compiuto un errore di configurazione nei propri router o non ha sufficiente capacità per trasportare il traffico. In stretta relazione con questo problema, c'è la necessità di fornire supporto per politiche molto flessibili nell'instradamento inter-dominio.

La soluzione a questo tipo di problema è il Border Gateway Protocol, che verrà presentato nella prossima sezione.

2.2 Soluzione, il BGP

Il Border Gateway Protocol[1] è un protocollo di rete usato per connettere fra loro router appartenenti a sistemi autonomi differenti, che vengono chiamati router gateway. È quindi un protocollo di routing inter-AS, nonostante possa essere utilizzato anche tra router appartenenti allo stesso AS (nel qual caso è indicato con il nome di iBGP, Interior Border Gateway Protocol)[1]. Il protocollo BGP si basa su un'ipotesi di partenza: Internet è un insieme di AS arbitrariamente interconnessi.

La funzione principale di un sistema BGP è quella di scambiarsi informazioni riguardanti la raggiungibilità di rete con altri sistemi BGP. Queste informazioni di raggiungibilità comprendono informazioni sull'elenco degli AS presenti, quali AS vengono attraversati da un percorso, l'identificativo dell'AS, ed altre informazioni utili, questi dati sono sufficienti per la costruzione di un grafo della connettività e raggiungibilità degli AS, dal quale possono essere eliminati cicli di routing, e dal quale possono essere prese decisioni politiche.

Le informazioni scambiate attraverso un sistema BGP, supportano solo il paradigma basato sulla destinazione d'inoltro, cioè che un router inoltra un pacchetto basato esclusivamente sull'indirizzo di destinazione presente nell'-header IP del pacchetto. Questo fatto riflette l'isieme delle decisioni politiche che possono, o no, essere eseguite utilizzando BGP. BGP inoltre fornisce un insieme di meccanismi per supportare il CIDR (Classless InterDomain Routing), una tecnica che risolve due problemi di scalabilità nella rete Internet: la crescita delle tabelle di instradamento per il backbone, per effetto della sempre maggiore quantità di numeri di rete che vi si deve memorizzare; e

[1] Anche se iBGP non è coerente con gli scopi principali del BGP

la possibilità che lo spazio di indirizzamento di IP venga esaurito. Questi meccanismi comprendono il supporto per la pubblicazione di una serie di destinazioni come prefissi IP, eliminando il concetto di classe di rete. BGP introduce anche altri meccanismi che consentono l'aggregazione di percorsi, tra cui l'aggregazione dei percorsi di AS[3].

2.2.1 Le caratteristiche del BGP

BGP è particolare per diversi aspetti, ma soprattutto non è un protocollo del vettore delle distanze e neppure un puro protocollo basato sullo stato dei collegamenti, ma annuncia la raggiungibilità di una determinata destinazione, invece che diffondere informazioni (costi, distanza) d'instradamento. BGP è un protocollo distribuito, nel senso che viene usato per comunicare solo con altri sistemi BGP, inquanto limita la distribuzione delle sue informazioni solo ai suoi pari. Inoltre questo protocollo segue la decentralizzazione, un concetto molto importante nell'ambito dei sistemi distribuiti, il quale indica il trasferimento del processo decisionale ad altri livelli di una gerarchia organizzativa. Infatti uno dei motivi del successo e della diffusione di BGP e che divide i meccanismi dalle scelte politiche. Di seguito elencheremo le principali caratteristiche del BGP.

- *Comunicazione tra sistemi autonomi.* Poichè è progettato come protocollo di gateway esterno, il suo ruolo principale è consentire ad un AS di comunicare con un altro.

- *Coordinamento tra più speaker BGP.* Se un sistema autonomo dispone di più router, ciascuno dei quali comunica con un altro router di un sistema autonomo esterno, può essere usata una forma di BGP, nota come *i*BGP, per coordinare i router nell'insieme, in modo che essi diffondano informazioni coerenti.

- *Diffusione delle informazioni di raggiungibilità.* BGP consente ad un sistema autonomo di annunciare le destinazioni raggiungibili al suo interno o attraverso esso, e apprendere tali informazioni da un altro sistema autonomo.

- *Paradigma del salto successivo.* Come i protocolli di instradamento basati sul vettore delle distanze, fornisce informazioni sul *salto successivo*[2] per ogni destinazione.

[2]Il salto successivo indica quale sarà il router successivo da attraversare prima che il pacchetto arrivi a destinazione

- *Supporto delle politiche.* Diversamente dalla maggior parte dei protocolli basati sul vettore delle distanze, che annunciano esattamente i percorsi da inserire nella tabella d'instradamento, BGP può implementare altre politiche scelte dall'amministratore locale. In particolare, un router che esegue BGP può distinguere tra l'insieme di destinazioni raggiungibili dai computer posti all'interno del suo AS, e l'insieme delle destinazioni annunciate ad altri AS.

- *Trasporto affidabile.* BGP si distingue dagli altri protocolli che trasportano informazioni d'instradamento, perchè si basa su un trasporto affidabile: perchè usa TCP[2] per le sue comunicazioni.

- *Informazioni d'instradamento.* Oltre a specificare le destinazioni che possono essere raggiunte e il salto successivo per ciascuna, gli annunci BGP includono informazioni d'instradamento, che consentono ad un destinatario di apprendere quali sistemi autonomi si trovano lungo il percorso verso la destinazione ed evitare cicli.

- *Aggiornamenti incrementali.* Per risparmiare la larghezza di banda della rete e la CPU dei router, non passa informazioni complete in ogni messaggio di aggiornamento. Queste vengono scambiate solo la prima volta e poi i messaggi successivi trasportano cambiamenti incrementali.

- *Supporto per indirizzamento senza classi.* BGP supporta gli indirizzi CIDR: cioè BGP invia una lunghezza del prefisso di rete insieme ad ogni indirizzo.

- *Aggregazione di rotte.* Risparmia la larghezza di banda della rete consentendo al mittente di aggregare le informazioni di instradamento e inviare una singola voce per rapprensentare più destinazioni correlate.

- *Autenticazione.* Consente al destinatario di autenticare i messaggi (cioè di verificare l'identità di un mittente).

2.2.2 Funzionamento

Per poter configurare il protocollo BGP ed effettuare lo scambio di informazioni riguardanti la raggiungibilità, il gestore di ciascun sistema autonomo sceglie almeno un nodo apposito (di solito un router di confine) e gli assegna la funzione di "annunciatore BGP" (BGP *speaker*), che si occuperà di iniziare, mantere e chiudere la connessione BGP con gli altri speaker, e di pubblicizzare gli annunci verso altri pari.

Oltre agli annunciatori BGP, ogni AS ha uno o più *gateway* di confine, che non coincidono necessariamente con gli annunciatori. I gateway di confine (*border gatway*) sono i router mediante i quali i pacchetti entrano ed escono dal sistema autonomo.

Al cuore di BGP ci sono gli annunci sui percorsi. Un annuncio consiste in un indirizzo di rete di destinazione in forma CIDR (es. 128.119.40/24), e un insieme di attributi associati al percorso verso la rete di destinazione. Vedremo successivamente com'è il formato dei messaggi scambiati.
Il funzionamento di BGP ruota intorno a tre attività, tutte legate agli annunci sui percorsi:

- *Ricezione e filtraggio di annunci sui percorsi da parte di vicini direttamente connessi.* Un router riceverà degli annunci sui percosi da parte di pari BGP. Possiamo pensare ad un annuncio su un percorso BGP come una "promessa". Un pari BGP che annuncia un percorso verso un AS di destinazione, promette che se un AS confinante gli rilancerà un datagram destinato a quel AS di destinazione, esso sarà in grado di inoltrare quel datagram lungo un percorso verso quella destinazione. Un router BGP può anche filtrare (scartare) gli annunci sui percorsi ricevuti. Per esempio, un router BGP ignorerà gli annunci che contengono il proprio numero di AS nell'AS–PATH, dato che quel percorso darebbe luogo ad un loop di instradamento, se usato. Poichè viene specificato l'intero percorso verso l'AS, un amministratore di rete può esercitare un notevole controllo sull'instradamento seguito dai datagram.

- *Selezione del percorso.* Un router BGP può ricevere diversi annunci sui percorsi verso lo stesso AS di destinazione, e deve scegliere quale percorso usare tra quelli annunciati. Tipicamente un router sceglierà solo uno dei diversi percorsi ricevuti, e dato che BGP fa una chiara distinzione tra meccanismo di instradamento e politica di instradamento, spetterà alla politica, e quindi all'amministatore e ai vari accordi che vengono presi tra i vari gestori, quale annuncio selezionare.

- *Invio di annunci sui percorsi ai vicini.* Così come un router BGP riceverà annunci sui percorsi dai suoi vicini, anche lui annuncerà percorsi ai suoi vicini. Ancora una volta BGP fornisce un meccanismo, ma non una politica, per questi annunci. Questo permette all'amministratore di rete un notevole grado di controllo sul traffico che sarà instradato attraverso la sua rete. Un BGP speaker publicizza agli altri speaker BGP solo i percorsi che esso utilizza.

Il flusso di dati inizialmente scambiato contiene la parte della tabella di routing BGP, consentita dalle varie politiche di esportazione, chiamata Adj-

Ribs-Out. Dato che BGP non richiede un aggiornamento periodico delle tabelle di routing, se avvengono cambiamenti sui percorsi di destinazione, verranno inviati successivi aggiornamenti delle tabelle. Per consentire cambiamenti di politica locale di avere l'effetto giusto senza ripristinare le connessioni BGP, uno speaker BGP deve o, mantenere l'attuale versione dei percorsi pubblicizzati per tutta la durata della connessione, o avvalersi del Route Refresh extension (che consente lo scambio dinamico degli aggiornamenti dei percorsi fra i vari BGP speakers e la successiva ri-pubblicazione dei rispettivi Adj-RIB-Out).

2.2.3 Percorsi: pubblicazione e memorizzazione

Un percorso è definito come un'unità di informazione, questi percorsi sono pubblicizzati dai BGP speaker in messaggi di aggiornamento (UPDATE). Percorsi multipli che hanno lo stesso attributo percorso possono essere pubblicizzati in un solo messaggio di UPDATE, inserendo più prefissi nel campo NLRI del messaggio di UPDATE. I percorsi sono memorizzati nel RIB (Routing Information Base): vale a dire, il Adj-RIB-In, la Loc-RIB e il Adj-RIB-out, come descritto successivamente. Se uno speaker BGP sceglie di pubblicizzare un percorso ricevuto in precedenza, esso potrà aggiungere o modificare l'attributo percorso relativo prima di pubblicare tale percorso agli speaker.

Il Routing Information Base (RIB)[1] all'interno di uno speaker BGP si compone di tre parti distinte:

- Adj-RIB-In: memorizza le informazioni di routing in entrata apprese dai messaggi di aggiornamento che sono stati ricevuti da altri speaker BGP. Il loro contenuto rappresenta itinerari che sono disponibili come input per il processo decisionale.

- Loc-RIB: contiene le informazioni di routing locale relative al BGP speaker, il quale applicherà le sue politiche locali per le informazioni di routing contenuti in sua Adj-RIB-In. Questi sono i percorsi che saranno utilizzati da parte dello speaker BGP locale.

- Adj-RIBs-Out: memorizza le informazioni del BGP speaker locale selezionato per la pubblicazione verso i suoi pari. Le informazioni di routing memorizzate nel Adj-RIBs-Out saranno inoltrate nei messaggi di aggiornamento del BGP speaker e pubblicizzati ai suoi pari.

In sintesi, Adj-RIB-In contiene informazioni di routing che sono state pubblicizzate allo speaker BGP locale dai suoi pari; Loc-RIB contiene i per-

corsi che sono stati selezionati dal processo decisionale dello speaker BGP locale, e Adj-RIBs-Out organizza le rotte per la pubblicazione verso speaker specifici (per mezzo di messaggi di aggiornamento).

Anche se il modello concettuale distingue tra Adj-RIB-In, Loc-RIB e Adj-RIB-out, questo non implica e né richiede che l'attuazione deve mantenere tre copie separate delle informazioni di routing. La scelta dell'implementazione (per esempio, 3 copie delle informazioni vs 1 copia con i puntatori) non è vincolata dal protocollo.

BGP prevede meccanismi mediante i quali uno speaker BGP può informare i suoi pari che un percorso precedentemente annunciato non è più disponibile per l'uso. Ci sono tre metodi con cui un dato speaker BGP può indicare che un percorso è stato ritirato dal servizio:

- Il prefisso che esprime l'IP di destinazione per un percorso precedentemente pubblicizzato può essere aggiunto nel settore PERCORSI RITIRATI nel messaggio UPDATE, segnando così il percorso associato come non più disponibili per l'uso.
- Un percorso di sostituzione con lo stesso NLRI può essere pubblicizzato.
- La connessione BGP speaker può essere chiusa, il quale implica la rimozione di tutte le rotte che la coppia di speaker aveva pubblicizzato l'un l'altro.

2.2.4 Formato messaggi

I peer che eseguono il protocollo BGP eseguono tre funzioni base.
La prima consiste nell'autenticazione e nell'acquisizione del partner iniziale: i due router stabiliscono una connessione TCP ed eseguono uno scambio di messaggi che garantiche che entrambi i lati siano d'accordo a comunicare.
La seconda costituisce l'elemento principale del protocollo: ciascun lato invia inforamzioni di raggiungibilità positive o negative, cioè un mittente può annunciare che una o più destinazioni sono raggiungibili, dando un salto successivo per ciascuna di esse, oppure può dichiarare che una o più destinazioni annunciate precedentemente non sono più raggiungibili.
La terza funzione, infine, permette di verificare che il partner e le connessioni stanno funzionando correttamente.
Per gestire le funzioni appena descritte, BGP definisce i seguenti tipi di messaggi base.

Bisogna premettere che un messaggio viene elaborato solo dopo che è stato interamente ricevuto, la dimensione massima dei messaggi è di 4096

ottetti (un ottetto indica un byte, otto bit), tutte le implementanzioni sono tenute a rispattare questa dimensione. Invece il più piccolo messaggio che può essere inviato è costituito da un header BGP senza una parte di dati (19 byte).

L'intestazione dei messaggi

Ciascun messaggio BGP inizia con un'instestazione fissa, che indica il tipo di messaggio, come mostrato in figura 2.1

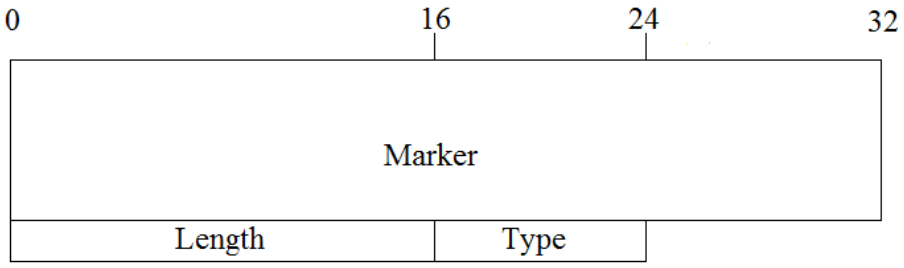


Figura 2.1: Header BGP

Il campo MARKER di 16 byte contiene un valore che entrambi i lati sono d'accordo di usare per contrassegnare l'inizio di un messaggio. A prima vista questo campo potrebbe sembrare insolito. Nel messsaggio iniziale il marcatore consiste in tutti i bit settati ad 1; se i peer BGP sono d'accordo nell'usare un meccanismo di autenticazione, il marcatore può contenere informazioni di autenticazione. In ogni caso, entrambi i lati devono essere d'accordo sul valore in modo che possa essere usato per la sincronizzazione. Per capire perchè la sincronizzazione è necessaria, si ricordi che tutti i messaggi BGP vengono scambiati attraverso un trasporto di flusso (cioè TCP) che non identifica il confine tra un messaggio e il successivo. In un ambiente di questo tipo, un semplice errore da entrambi i lati può avere conseguenze drammatiche. In particolare, se il mittente o il destinatario sbagliano il conteggio dei byte in un messaggio, si verificherà un errore di sincronizzazione. Poichè non specifica i confini di un messaggio, il protocollo di trasporto non avviserà il destinatario dell'errore. Per essere certi che il mittente e il destinatario rimangano sincronizzati, quindi, BGP pone una sequenza ben nota

all'inizio di ciascun messaggio e richiede che un destinatario verifichi che il valore sia corretto prima di elaborare il messaggio.

Il campo LENGTH di 2 byte specifica la lunghezza totale in byte del messaggio, compresa l'intestazione. Quindi permette di individuare il campo MARKER del messaggio successivo nel flusso TCP. Il valore di questo campo deve sempre essere almeno di 19 byte e non superiore di 4096.

Il campo TYPE di 1 byte indica il codice del tipo di messaggio che sta per essere spedito, di seguito i quattro tipi di codice:

1. OPEN
2. UPDATE
3. NOTIFICATION
4. KEEPALIVE

Formato del messaggio OPEN

Dopo che è stata stabilita una connessione, il primo messaggio inviato da ogni lato della comunicazione è un messaggio di OPEN, in aggiunta alla dimensione gia fissata dell'header, un messaggio OPEN contiene i seguenti campi, mostrati nella figura: 2.2

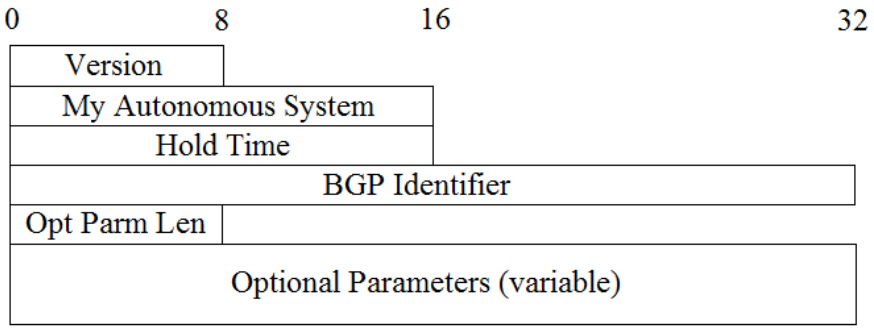


Figura 2.2: Formato messaggio OPEN

Il campo Version è rappresentato da un intero senza segno delle dimensioni di 1 byte, ed indica il numero della versione del protocollo utilizzato, in questo caso la versione è 4 (BGP-4).

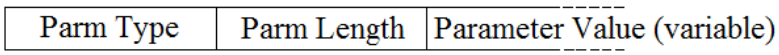
My Autonomous System è rappresentato da un intero senza sengno di dimensione pari a 2 byte, ed indica il numero dell'AS del mittente.

Hold Time, un intero senza segno di 2 byte, indica il numero di secondi che il mittente propone con valore di Holt Timer. Su ricevimento di un messaggio di OPEN, uno speaker BGP deve calcolare il valore dell'Hold Timer usando il più piccolo tra i valori di Holt Time da lui configurato, o da quello appena ricevuto nel messaggio di OPEN. Un'implementazione corretta dovrebbe chiudere la connessione in base a questo valore, che dovrebbe essere compreso tra i zero e tre secondi. Il valore calcolato indica il massimo numero di secondi che dovrebbero trascorrere tra la ricezione di un messaggio KEEPALIVE o UPDATE e il successivo.

BGP Identifier, un intero senza segno di 4 byte che indica l'identificativo BGP del mittente, è lo stesso speaker BGP che setta questo valore del suo campo. Questo valore viene determinato fin dall'inizio della creazione del BGP speaker, e sarà sempre lo stesso per ogni comunicazione.

Optional Parameters Length, questo intero senza segno di 1 byte, indica la lunghezza in byte del campo Optional Parameters. Se il valore di questo campo è zero, il campo Optional Parameters non sarà presente.

Optional Parameters, il campo contiene una lista di parametri opzionali, il quale ogni parametro è formato da una tripla codificato nel seguente modo:



Parameter Type è un campo di 1 byte che identifica in modo non ambiguo i parametri individuali.

Parameter Length è un campo di 1 byte contenente la lunghezza in byte del campo Parameter Value.

Parameter Value è un campo di lunghezza variabile che viene interpretato secondo il valore del campo Parameter Type.

La lunghezza minima del messaggio OPEN è di 29 byte, inclusa l'intestazione.

Formato del messaggio UPDATE

I messaggi di UPDATE vengono utilizzati per trasferire informazioni di routing tra speaker BGP. Le informazioni contenute nel messaggio UPDATE possono essere usate per costruire un grafico che descrive le relazioni dei vari

Autonomous System. Applicando le politiche che dovranno essere discusse, le informazioni riguardanti i cicli di routing e alcune altre anomalie possono essere individuate e rimosse dall'instradamento inter-AS.

Un messaggio di UPDATE viene utilizzato per pubblicizzare percorsi fattibili, oppure ritirare le rotte che non sono più praticabili. Un messaggio di UPDATE può allo stesso tempo sia pubblicizzare un percorso, che ritirare altri in disuso dal servizio. Come sempre insieme a questo messaggio è inclusa l'intestazione, la figura 2.3 ci mostra il formato di questo messaggio.

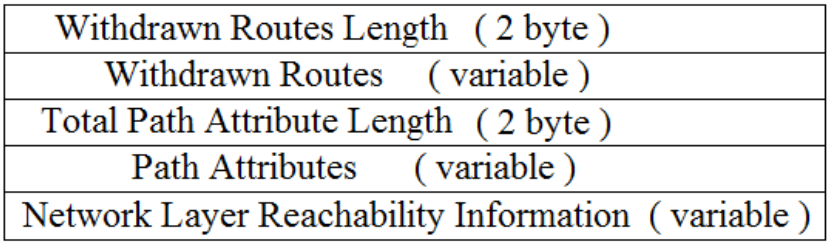
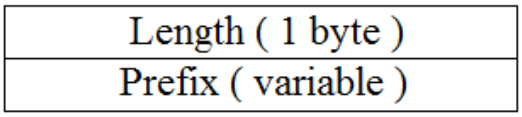


Figura 2.3: Formato messaggio UPDATE

Il campo Withdrawn Routes Length viene rappresentato da un intero senza segno di 2 byte ed indica la lunghezza totale in byte del campo Withdrawn Routes. Il valore 0 indica che non vi sono percorsi da ritirare dal servizio, e che il campo Withdrawn Routes non è presente in questo messaggio UPDATE.

Il Withdrawn Routes è un campo di lunghezza variabile che contiene un elenco dei prefissi di indirizzi IP per i percorsi che vengono ritirati dal servizio. Ogni prefisso IP è codificato nella tupla mostrata di seguito



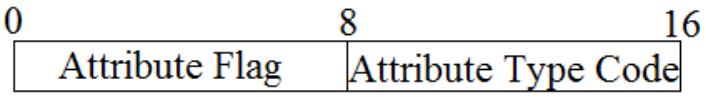
Il campo Length indica la lunghezza in bit del prefisso dell'indirizzo IP. Una lunghezza pari a zero indica un prefisso che corrisponde a tutti gli indirizzi IP.

Il campo Prefix contiene un prefisso di indirizzo IP, seguito dal numero minimo di bit finali necessari per delimitare la fne del campo, il valore finale di questi bit è irrilevante.

Il campo Total Path Attribute Length è rappresentato da un intero senza segno di 2 byte ed indica la lunghezza in byte del campo Path Attribute. Il suo valore permette di determinare la lunghezza del campo Network Layer Reachability Information (NLRI), e se il suo valore è uguale a zero, né il campo NLRI, né Path Attribute sono presenti.

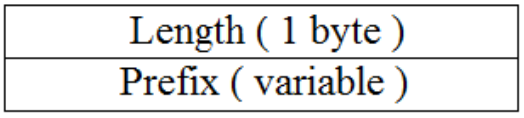
Il Path Attributes è un campo di lunghezza variabile di attributi percorso, ed è presente in ogni messaggio di UPDATE, ad eccezione di un messaggio di aggiornamento che porta solo il ritiro di alcuni percorsi. Ogni attributo percorso è formato dalla tripla <attribute type, attribute length, attribute value>.

Attribute Type è un campo di 2 byte, che consiste a sua volta di un campo di 1 byte che rappresenta Attribute Flag, e l'altro indica Attribute Type Code, come mostrato di seguito:



In base a come sono settati i bit all'interno di questi due campi, si posso reperire informazioni molto importati riguardo: l'origine del percorso, se è stato originato all'interno di un AS, o ricevuto da un altro AS; l'isieme degli AS attraversati e l'ordine in cui sono presenti nel percorso; l'indirizzo IP del router che dovrebbe essere utilizzato con salto successivo verso le destinazioni elencate nel NLRI.

Il Network Layer Reachability Information è un campo di lunghezza variabile che racchiude una lista di prefissi IP. Le informazioni di raggiungibilità sono codificate come una o più tuple nella forma seguente:



Il campo Length indica la lunghezza in bit del prefisso dell'indirizzo IP. Una lunghezza pari a zero indica un prefisso che corrisponde a tutti gli indirizzi IP.

Il campo Prefix contiene un prefisso di indirizzo IP, seguito dal numero minimo di bit finali necessari per delimitare la fne del campo, il valore finale di questi bit è irrilevante.

La lunghezza minima di un messaggio di UPDATE è di 23 byte, di cui 19 fanno parte dell'header del messaggio, più 2 per il Withdrawn Routes Length e gli altri 2 per il Total Path Attribute Length.

Formato del messaggio NOTIFICATION

Un messaggio di notifica viene inviato quando viene rilevata una condizione di errore, di conseguenza la connessione BGP verrà chiusa subito dopo l'invio di questo messaggio. In aggiunta all'hearder BGP, il messaggio NOTIFICATION è mostrato nella figura 2.4

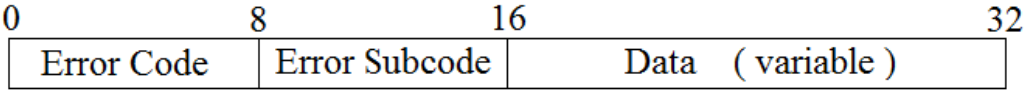


Figura 2.4: Formato messaggio NOTIFICATION

Il campo Error Code rappresentato da un intero senza segno di 1 byte indica il tipo di notifica, in base ai codici di errori elencati di seguito:

1. Message Header Error
2. OPEN Message Error
3. UPDATE Message Error
4. Hold Timer Expired
5. Finite State Machine Error
6. Cease

Il campo Error subcode rappresentato da un intero senza segno di 1 byte, fornisce informazioni più specifiche riguardanti la natura dell'errore segnalato. Ogni codice di errore può avere uno o più sottocodici ad esso assiociati.

Il campo Data, di dimensioni variabili è usato per diagnosticare il motivo della notifica, il suo contenuto dipende dal codice e dai sottocodici di errore.

Formato del messaggio KEEPALIVE

Questo tipo di messaggio viene inoltrato per verificare la raggiungibilità di altri speaker BGP, viene scambiato tra pari BGP molto spesso, prima che scada l'Hold Timer, per tenere ancora viva la connessione. Un tempo massimo ragionevole tra un messaggio KEEPALIVE e l'altro è di un secondo, anche se in base al valore dell'Hold Timer si può implementare un frequenza maggiore per l'invio di questi messaggi. Un messaggio KEEPALIVE consiste solo dell'intestazione BGP, che ha una dimensione di 19 byte.

2.2.5 Automa a stati finiti

I peer BGP usano un semplice automa a stati finiti[13], Finite State Machine (FSM)[1], per prendere le decisioni che riguardano l'interazione con altri peer BGP. L'automa è composto da sei stati:

- Idle (Inattiva)
- Connect (Connetti)
- Active (Attivo)
- OpenSent (Apertura Inviata)
- OpenConfirm (Apertura Confermata)
- Established (Stabilito)

Ciascun peer BGP attraversa gli stati descritti quando cerca di stabilire e mantenere in vita una sessione con un altro peer.
BGP deve mantenere una FSM separato per ogni peer configurato. Ogni peer BGP accoppiato in una potenzizale connessione proverà a connettersi all'altro, a meno che non sia configurato per rimanere nello stato IDLE, o configurato per rimanere passivo. Il lato attivo o la fase di collegamento della connessione TCP (il lato di una connessione TCP inviando il primo pacchetto TCP SYN) viene chiamata in uscita. Il lato passivo o di ascolto (il mittente del primo SYN/ACK) è chiamata connessione in entrata.
Un connessione BGP deve collegarsi e ascoltare sulla porta 179 della connessione TCP per le connessioni in entrata, oltre a cercare di connettersi ad altri pari. Esiste un periodo in cui è nota l'identità del peer all'altra estremità di una connessione in entrata, ma l'identificatore BGP non è noto, durante questo periodo, sia una connessione in entrata che in uscita possono esistere per lo stesso peer configurato. Questa operazione viene definita come una collisione di collegamento.

Un implementazione BGP avrà, al massimo, uno stato FSM configurato per ogni peer, più uno stato FSM per ciascuna connessione TCP in ingresso per i quali il peer non è stato ancora identificato. Ogni FSM corrisponde esattamente ad una connessione TCP. Ci possono essere più connessioni tra una coppia di peer se le connessioni sono configurate per utilizzare un paio di indirizzi IP differenti.

Gli attriburi necessari per ciascuna connessione sono:

1. Stato

2. ConnectRetryCounter
3. ConnectRetryTimer
4. ConnectRetryTime
5. HoldTimer
6. HoldTime
7. KeepaliveTimer
8. KeepaliveTime

L'attributo Stato indica lo stato corrente dello speaker BGP, ConnectRetryCounter indica il numero di volte che un peer BGP ha cercato di stabilire una connessione.

Invece questi attributi opzionale elencati di seguito possono essere sia supportati per connessioni esterne che per sistemi locali.

1. AcceptConnectionsUnconfiguredPeers
2. AllowAutomaticStart
3. AllowAutomaticStop
4. CollisionDetectEstablishedState
5. DampPeerOscillations
6. DelayOpen
7. DelayOpenTime
8. DelayOpenTimer
9. IdleHoldTime
10. IdleHoldTimer
11. PassiveTcpEstablishment
12. SendNOTIFICATIONwithoutOPEN
13. TrackTcpState

Le parole attivo e passivo hanno significati leggermente diversi quando applicati a connessioni tcp o a peer. C'è solo un lato attivo ed uno passivo ad ogni connessione TCP. Quando uno speaker BGP è configurato come attivo, può finire sia sul lato attivo che su quello passivo della connessione che viene eventualmente stabilita. Una volta che la connessione TCP è stata completata, non importa quale sia il ruolo dello speaker BGP, se quello passivo o attivo, l'aspetto più importante è che ci sia una connessione TCP sulla porta 179.

Stato Idle

Inizialmente lo stato FSM di ogni speaker BGP è impostato nello stato Idle, in questo stato vengono rifiutate tutte le connessioni in entrata per questo peer BGP. In risposta alla manifestazione dell'evento di inizio connessione (avviata da entrambi i sistemi), il sistema locale inizializza tutte le risorse BGP, avvia il timer ConnectRetry, inoltre avvia una connessione di trasporto verso altri peer BGP. Mentre è in ascolto sulla connessione, che può essere avviata dal peer BGP remoto, cambia il suo stato di Connect. Il valore esatto del timer ConnectRetry è una questione locale, ma dovrebbe essere sufficiente a consentire l'inizializzazione dell connessione TCP.
Un altro evento che crea cambiamenti dello stato Idle e PassiveTcpEstablishment, manuale o atomatico, questo attributo opzionale indica il fatto che il peer ascolterà prima di stabilire una connessione. In risposta al verificarsi di questi eventi, il sistema inizializza tutte le risorse BGP, setta il ConnectRetryCounter a zero, imposta il ConnectRetryTimer al valore iniziale, rimane in ascolto per una connessione che potrebbe essere iniziata da un peer remoto, e infine cambia lo stato in Active.
Ogni altro evento ricevuto quando il sistema è Idle non causa nessun cambiamento nello stato del sistema locale.

Stato Connect

In questo stato, il peer è in attesa che la connessioen TCP sia stata completata.

Se la connessione è andata a buon fine, se scade il timer opzionale DelayOpenTimer, oppure l'attributo DelayOpen è settato a FALSE, il sistema cancella il ConnectRetryTimer, completa l'inizializzazione, manda un messaggi di OPEN ai suoi pari, imposta HoldTimer ad un valore elevato e cambia il suo stato in OpenSent.
Se il collegamento al protocollo di trasporto fallisce (ad esempio, timeout

in ritrasmissione), il sistema locale riavvia il timer ConnectRetry, continua ad ascoltare per una connessione che potrebbe essere avviata dal peer BGP remoto, e cambia il suo stato in Active.
In risposta allo scadere del timer ConnectRetry, il sistema locale, chiude la connessione, riavvia il timer ConnectRetry, avvia una connessione di trasporto verso altri peer BGP, continua ad ascoltare per una connessione che potrebbe essere avviata dal peer BGP remoto, e rimane nello stato Connect.
In caso il controllo all'intestazione del messaggio BGP, o al messaggio OPEN, rileva un errore, oppure viene ricevuto un messaggio di tipo NOTIFICATION, o la connessione è stata chiusa manualmente e in risposta a qualsiasi altro evento, il sistema locale rilascia tutte le risorse BGP associate, successivamente taglia la connessione e cambia il suo stato di Idle.
Quando invece accadono eventi di "start" , questi vengono ignorati.
Infine se un messaggio di OPEN viene ricevuto mentre il DelayOpenTimer sta scorrendo, il sistema ferma il DelayOpenTimer e lo setta a zero, completa l'inizializzazione BGP, spedisce un messaggio OPEN, spedisce un messaggio KEEPALIVE, e cambia il suo stato in OpenConfirm.

Stato Active

In questo stato BGP sta cercando di acquisire un peer per iniziare una connessione TCP.

Se avviene un evento di chiusura connessione, o vengono rilevati errori nell'header del messaggio o in un messaggio di OPEN, se viene ricevuta una notifica di errore da parte del BGP, o se il DelayOpenTimer non sta scorrendo, o in risposta ad ogni altro evento, il sistema locale resetta tutti gli attributi Timer, rilascia tutte le risorse BGP associate, chiude la connessione e cambia il suo stato in Idle.
Se la connessione di livello trasporto riesce, o il DelayOpenTimer scade o se l'attributo DelayOpen è settato a FALSE, il sistema setta i valori dei rispettivi timer, completa l'inizializzazione, invia un messaggio OPEN ai suoi pari e cambia il suo stato in OpenSent
In risposta allo scadere del ConnectRetryTimer, il sistema locale riavvia il timer ConnectRetry, avvia una connessione di trasporto verso altri peer BGP, continua ad ascoltare per una connessione che potrebbe essere avviata da un peer remoto, e cambia il suo stato di Connect.
Se il sistema locale rileva che un peer remoto sta tentando di stabilire una connessione BGP ad esso, e l'indirizzo IP del peer remoto non è atteso, o se la connessione TCP ha avuto successo, il sistema locale riavvia il timer ConnectRetry, respinge il tentativo di connessione, continua ad ascoltare per

un connessione che potrebbe essere avviata dal peer remoto, e rimane nello stato Active.
Se invece accadono eventi di "start" , questi vengono ignorati.

Stato OpenSent

In questo stato lo speaker BGP attende un messaggio OPEN dal suo peer.

Se viene chiusa manualmente o automaticamente la connessione, se scade il timer HoldTimer, se vengono rilevati errori nell'header del messaggio o in un messaggio di OPEN, se viene ricevuto un messaggio NOTIFICATION o avviene una collisione nella connessione, il sistema spedisce un messaggio di notifica, setta i vari attributi riferiti ai timer, rilascia tutte le risorse BGP, chiude la connessione ed imposta il suo stao in Idle.
Se non ci sono errori rilevati nella ricezione del messaggio OPEN, BGP invia un messaggio KEEPALIVE e imposta un timer KeepAlive. Hold Timer, che in origine era impostata su un valore elevato, viene sostituito con il valore negoziato Hold Time se questo valore è zero, allora il timer Hold Time e timer KeepAlive non vengono avviati. Se il valore del campo Autonomous System è lo stesso del numero di sistema autonomo locale, la connessione è una connessione interna, altrimenti, è esterna. Infine, lo stato viene modificato in OpenConfirm.
Se una notifica di disconnessione viene ricevuta dal protocollo di trasporto sottostante, il sistema locale chiude la connessione BGP, riavvia il timer ConnectRetry, mentre continua l'ascolto per la connessione che potrebbe essere avviata dal peer remoto, e va nello stato Active.
Come nei casi precedenti se accadono eventi di "start" , questi vengono ignorati.

Stato OpenConfirm

In questo stato lo speaker BGP è in attesa di ricevere un messaggio di tipo KEEPALIVE o NOTIFICATION.

Se la connessione viene interrotta manualmente o in modo automatico, se l'HoldTimer scade, se la connessione viene interrota a livello trasporto, o viene ricevuto un messaggio di notifica da parte dei peer BGP, o vengono rilevati errori nell'header del messaggio o in OPEN, oppure collisioni, e in risposta ad ogni altro evento, il sistema locale invia un messaggio NOTIFICATION, rilascia tutte le risorse BGP, setta il ConnectRetryTimer a zero, chiude la connessione corrente e cambia il suo stato in Idle.

Se scade il KeepaliveTimer, il sistema invia un messaggio di KEEPALIVE, riavvia il timer e rimane nello stato OpenConfirm.
Se il sistema locale riceve un messaggio KEEPALIVE, riavvia HoldTimer e cambia il suo stato in Established.

Stato Established

Nello stato di Established BGP può scambiare UPDATE, NOTIFICATION, e messaggi KEEPALIVE con i suoi pari.

Se viene chiusa manualmente o automaticamente la connessione, se scade HoldTimer, se vengono rilevate collisioni, ricevuti messaggi di notifica, se viene ricevuto un messaggio UPDATE contenente errori, o si verifica ogni altro evento, il sistema locale invia un messaggio di notifica, rilascia tutte le risorse BGP, taglia la connessione e cambia il proprio stato in Idle.
Se il sistema locale riceve un messaggio KEEPALIVE o UPDATE, processa il messaggio di UPDATE, riavvia HoldTimer e rimane nello stato Estblished.
Se il timer KeepAlive scade, il sistema locale invia un messaggio KEEPALIVE e riavvia il suo timer KeepAlive. Ogni volta che il sistema locale invia un messaggio KEEPALIVE o UPDATE, si riavvia il suo timer KeepAlive, a meno che il valore Hold Time negoziato è zero.

Capitolo 3

Sicurezza nel BGP

In questo capitolo affronteremo i temi che riguardano i meccanismi di sicurezza forniti da questo protocollo. È evidente che Internet è vulnerabile agli attacchi attraverso i suoi protocolli di routing e BGP non fa eccezione. Difetti, errori di configurazione, attacchi espliciti sono fonti di disturbo per il comportamento globale di Internet, inserendo informazioni di routing errate nella rete, qualsiasi interruzione nella comunicazione ha un effetto a catena su tutto il routing. Meccanismi di autenticazione e crittografa non sono parte integrante del protocollo. Come il protocollo TCP/IP, anche il BGP è soggetto agli stessi attacchi, a causa della mancanza di un mezzo sicuro di verifica dell'autenticità e leggittimità del traffico BGP. Questi limiti presentati dal protocollo contribuiscono all'instabilità della rete globale.

BGP non è in grado di proteggere l'integrità la freschezza e l'originale autenticità dei messaggi, non è in grado di validare l'autorità di un AS quando annuncia determinate informazioni, non assicura l'autenticità degli attributi contenuti in un determinato percorso annunciato da un AS. Ad oggi nessuna soluzione concreta è largamente utilizzata per garantire queste proprietà, la scelta delle politiche di sicurezza viene lasciata ai singoli AS.

BGP può essere soggetto a violazioni di confidenzialità, non prevede la protezione contro la riproduzione dei suoi messaggi, così come l'iserimento, la cancellazione, e la modifica di essi, è soggetto a man-in-the-middle attack, e i danni che potrebbero derivare da questi attacchi sono:

- Starvation: i dati del traffico destinato ad un nodo vengono inoltrati per una parte in una rete che non può consegnarli.
- La congestione della rete: se in una rete arriva più traffico il quale non riesce a trasportare.

- Blackhole: grande quantità di traffico sono destinate ad essere trasmesse attraverso un router che non può gestire l'aumento del livello di traffico.
- Ritardo: il traffico dati destinato ad un nodo è trasmesso lungo un percorso che è in qualche modo inferiore al percorso che dovrebbe prendere.
- Looping: il traffico dati viene trasmesso lungo un percorso con cicli, in modo che i dati non vengono mai consegnati.
- Eavesdrop: il traffico dati viene trasmesso attraverso alcuni router o reti sbagliate, offrendo l'opportunità di intercettare i dati.
- Partizione: una certa parte della rete ritiene che è separata dal resto dell'altra rete, quando, in realtà, non lo è.
- Taglio: una certa parte della rete ritiene che non abbia rotta per qualche rete a cui essa è, di fatto collegata.
- Churn: il forwarding nella rete cambia a un ritmo elevato, determinando notevoli differenze nei modelli di consegna dei dati.
- Instabilità: BGP diventa instabile in modo che la convergenza su uno stato globale di spedizione non è conseguita.
- Sovraccarico: i messaggi BGP stessi diventano una parte significativa del traffico della rete.
- Esaurimento delle risorse: i messaggi BGP stessi causano un esaurimento delle risorse dei router, come lo spazio nelle tabelle, e CPU.
- Address-spoofing: il traffico dati è trasmesso attraverso alcuni router o reti legate allo spoofing, permettendo così un attacco attivo, in quanto consentono la possibilità di modificare i dati.

Non sono solo gli attacchi espliciti a procurare i danni appena elencati, ma un'altra causa sono gli errori di configurazioni, che si dividono in due forme tipiche:

- Exports misconfiguration: cioè che un router esporta un percorso che in realtà deve solo filtrare.
- Origin misconfiguration: cioè un AS inserisce un prefisso errato nelle tabelle globali.

3.1 S-BGP

Uno dei primi meccanismi implementati è il Secure Border Gateway Protocol (S-BGP)[8], che utilizza la potenza della crittografia a chiave pubblica e dei certificati digitali. L'approccio adottato per assicurare la distribuzione dei persorsi attraverso il BGP prevede due infrastrutture a chiave pubblica (Public Key Infrastructures, PKI), un nuovo attributo percorso contenente attestati, e l'utilizzo di IPsec. Queste componenti sono utilizzate da un BGP speaker per convalidare l'autenticità e l'integrità dei messaggi di UPDATE che esso riceve, e per verificare l'identità e l'autorizzazione dei mittenti.

In primo luogo un PKI viene utilizzato per supportare l'autenticazione della "proprietà" di una porzione dello spazio di indirizzamento IP. Questo certificato è rilasciato dalla stessa entità che è responsabile anche dell'assegnazione degli indirizzi.
La seconda infrastruttura a chiave pubblica viene utilizzata per autenticare l'assegnazione di un numero associato ad un AS, l'identità di un router BGP e la sua autorizzazione a rappresentare un AS. Queste informazioni riguardanti i certificati e le le firme digitali, vengono memorizzate in un campo del messaggio UPDATE.
Infine il protocollo IPsec fornisce i servizi di sicurezza necessari da parte dello speaker BGP ricevente di verificare l'integrità del messaggio, l'identità del mittente, e il fatto che esso sia il destinatario di ogni messaggio. I messaggi dei vari router vengono firmati dalla chiave privata e autenticati dagli altri con quella pubblica, purtroppo il sistema è dispendioso in tempo e calcolo vista l'entità delle macchine presenti. Tuttavia, uno dei principali ostacoli alla diffusione di S-BGP è che richiede la partecipazione di numerose organizzazioni distinte: fornitori di router, fornitori di servizi Internet (ISP), e enti internazionali (ICANN).

3.2 Listen e Whisper

Per ridurre la vulnerabilità del BGP, esistono anche questi due meccanismi: *Listen* e *Whisper*[12].
Listen sonda passivamente il piano dati e verifica i percorsi di base per diverse destinazioni. Whisper utilizza funzioni di crittografia insieme con routing ridondante per rilevare falsi annunci di rotte nel piano di controllo. Questi meccanismi sono facilmente rimovibili e non fanno affidamento né ad un'infrastruttura a chiave pubblica né ad un'autorità centrale come ICANN. La combinazione di Listen e Whisper elimina un gran numero di problemi dovuti per errori di configurazione del router, e limita (anche se non elimina) i danni

che possono causare attacchi intenzionali. Inoltre, questi meccanismi sono in grado di rilevare e contenere gli attacchi isolati che si propagano anche su qualche annuncio di percorso valido.

3.2.1 Whisper

Descriveremo il protocollo Whisper, un piano di verifica tecnica di controllo che propone modifiche minori al BGP, per aiutare ad individuare percorsi non validi da router mal configurati. Whisper fornisce le seguenti proprietà:

- Se ogni router mal configurato o non autorizzato propaga un percorso non valido, verrà sempre innescato un meccanismo di allarme.
- Se un singolo router mal configurato pubblicizzerà più di un paio di percorsi non validi, essi saranno rilevati, e gli effetti di quei percorsi saranno limitati.

Il modello utilizzato da Whisper è quello di considerare due percorsi diversi per la stessa destinazione e verificare se siano coerenti fra di loro. Un nodo destinazione fa un controllo di coerenza in base al campo AS_PATH, quando viene rilevata un'incoerenza il protocollo è in grado di stabilire che almeno uno dei due non è valido. Tuttavia, non si può chiaramente individuare l'origine della rotta invalida.

3.2.2 Listen

Il protocollo Listen, un piano di verifica tecnica dei dati che rileva problemi di raggiungibilità nel piano dati e li segnala.
L'idea generale di Listen è di monitorare i flussi TCP, e di trarre conclusioni sullo stato di un percorso da queste informazioni. Il percorso di instradamento in avanti e indietro tra due end-host può essere diverso. Così possiamo osservare il flusso di pacchetti in una sola direzione.

La differenza principale con un meccanismo come S-BGP, è che Listen e Whisper non cercano di individuare e risolvere il problema, ma cercano di individuarlo e segnalarlo.

3.3 Firma MD5

Un altro modo per rendere più affidabile la sessione BGP, è puntare a rendere più sicuro il protocollo di trasporto a cui si appoggia, il TCP. Si usa

MD5 (un algoritmo di hash)[17] che codifica l'header del pacchetto TCP. La motivazione principale per questa opzione è quella di consentire al BGP di proteggersi contro l'introduzione di segmenti di spoofing TCP nel flusso di connessione.

Ogni segmento inviato su una connessione TCP, per essere protetto contro lo spoofing, dovrà contenere il digest (firma) MD5 di 16 byte prodotta applicando l'algoritmo MD5 per questi elementi nel seguente ordine:

1. Lo pseudo-header TCP (nell'ordine: indirizzo IP sorgente, indirizzo IP di destinazione, campo pad a zero, e la lunghezza del segmento).

2. L'header TCP, ad esclusione delle opzioni, e assumendo un checksum pari a zero.

3. I dati del segmento TCP (se presenti).

4. Una chiave indipendente specificata o una password, nota ad entrambi e presumibilmente specifica per quella connessione.

La natura della chiave è lasciata indeterminata, ma deve essere conosciuta da entrambi i lati della connessione. Alla ricezione di un segmento firmato, il ricevitore deve validare, calcolando il proprio digest dagli stessi dati (utilizzando la propria chiave) e confrontando i due digest.

3.4 Pretty Secure BGP

Pretty secure BGP (psBGP)[16] si avvale di un modello di fiducia centralizzato per l'autenticazione dei numeri relativi agli AS, e un modello di fiducia decentralizzato per la verifica della correttezza del prefisso IP di origine. Seguendo l'esempio di S-BGP, psBGP fa uso di un sistema centralizzato, PKI, per autenticare il numero associato ad un AS, attraverso le quattro autorità di certificazione (CA) corrispondenti ai quattro RIR (Regional Internet Registry) esistenti. In psBGP per certificare l'autenticità di uno speaker BGP, viene assegnata ad un AS, a cui è gia stato assegnato un numero univoco, una chiave pubblica, condivisa da tutti gli speaker appartenti a quell'AS, questa chiave pubblica viene chiamata SpeakerCert. Questa SpeakerCert viene firmata da uno speaker BGP con la sua chiave privata, quindi una SpeakerCert possiamo vederla come un'affermazione fatta da un AS, che uno speaker BGP con la sua chiave privata è autorizzato a rappresentare quel AS. La chiave privata corrispondente alla chiave pubblica di un SpeakerCert viene utilizzata per stabilire connessioni sicure con gli altri peer, e per la firma

dei messaggi BGP. Per garantire l'integrità dei dati, come S-BGP e SoBGP, si utilizzano le funzionalità fornite dal protocollo IPSec, usando ESP (Encapsulating Security Payload), che ha l'obiettivo di fornire confidenzialità e controllo di integrità e autenticità alla comunicazione.

3.5 Altri meccanismi di siscurezza

3.5.1 GTSM (Generalized TTL Security Mechanism)

(GTSM)[15] è stato progettato per proteggere un router TCP / IP da attacchi basati su utilizzazione della CPU. Con questa tecnica molti attacchi basati sul sovraccarico della CPU possono essere prevenuti con il semplice meccanismo descritto in questo paragrafo. GTSM si basa sul fatto che la stragrande maggioranza delle comunicazioni sono stabilite tra router adiacenti. Dal momento che lo spoofing (falsificazione) TTL è considerato quasi impossibile, un meccanismo basato su un valore di TTL previsto è in grado di fornire una difesa semplice e ragionevolmente solida da attacchi basati su pacchetti di protocollo falsi. Il funzionamento è semplice, il campo TTL, che determina il numero massimo di router che possono essere attraversati da un pacchetto, dell'header del protocollo IP, è settato a 255, il router che riceve il pacchetto controlla il campo, dato che tra i due router non dovrebbero esserci altri dispositivi, se il valore è minore di 254 il pacchetto è stato alterato e viene scartato.

3.5.2 Registri di routing

Sono dei depositi centralizzati di informazioni riguardanti le politiche di routing, vengono memorizzate inoltre anche informazioni topologiche della rete. Il difetto di questi registri sta nella lentezza nelle query e nell'aggiornamento delle informazioni. Utilizzare un registro significa assumere che il registro stesso sia sicuro, e questo è impossibile da garantire.

3.5.3 SoBGP (Secure Origin Boarder Gateway Protocol)

La parola chiave di questa architettura è flessibilità, cioè che ogni amministratore di un AS può impostare il grado di sicurezza che ritiene più adeguato. Questo architettura è simile al S-BGP, che utilizza i certificati per

garantire l'autenticità dei messaggi e delle associazioni, con la differenza che vengono usati tre PKI per gestire:

- l'associazione tra chiave e speaker SoBGP;
- l'associazione tra la chiave, le politiche e la topologia di rete;
- l'associazione tra chiave e indirizzi di AS.

Le informazioni appena elencate vengono trasmesse attraverso un nuovo messaggio: SECURITY BGP, e viene impiegato un database topologico per convalidare le informzioni di routing. I messaggi di UPDATE che violano queste informazioni vengono scartati.
Per aumentare le prestazioni di questo sistema, si predilige l'autenticazione a lungo termine (relazioni tra AS, topologie, ecc.) così da pre-caricare i dati prima della vera sessione BGP.

3.5.4 IRV (Interdomain Route Validation)

IRV è un sistema che utilizza una sua architettura e un suo portocollo dedicato, a differenza di S-BGP non intacca assolutamente il protocollo di routing.
Il funzionamento è semplice, vengono utilizzati dei server IRV dedicati per ogni AS, alla ricezione di un messaggio di UPDATE, un router interroga il server IRV locale per chiedere la correttezza del messaggio, il quale si preoccuperà di reperire le informazioni da altri server IRV di altri AS. Saranno poi le politiche del router a decidere se convalidare o rifiutare il messaggio ricevuto.
Questo tipo di meccanismo è computazionalmente caro, dato l'impiego di server dedicati per ogni AS e di un protocollo apposito per la loro comunicazione, ma è molto più sicuro e gestibile dei registri di routing.

Di seguito viene mostrata una tabella che sintetizza il rapporto che c'è fra i livelli di sicurezza e le soluzioni appena descritte.

SOLUZIONI			SERVIZI DI SICUREZZA		
Sistema	***In uso***	***Tipologia***	***Aut. Topologica***	***Aut. Percorso***	***Aut. Origine***
Route filtering	SI	anomaly	debole	debole	debole
Registri routing	SI	anomaly	debole	debole	debole
S-BGP	NO	crypto	forte	forte	forte
SoBGP	NO	crypto/anomaly	forte	nessuna	forte
IRV	NO	crypto/anomaly	forte	forte	forte
psBGP	NO	crypto	nessuna	nessuna	forte
Listen Protocol		anomaly	nessuna	nessuna	debole

Figura 3.1: -crypto: viene usato un sistema crittografico
-anomaly: il sistema si basa sul riconoscimento di anomalie nei dati che elabora

Capitolo 4

Analisi del BGP

Quando parliamo di un protocollo in generale, in questa tesi del BGP, per valutare l'efficienza, l'affidabilità, quali sono i pregi e i difetti, bisogna tener conto di diversi aspetti.
Uno di questi è la sicurezza, discussa nel capitolo precendente, il quale si occupa di garantire l'integrità dei messaggi, l'autenticazione, sia dei pari BGP che dei messaggi, la confidenzialità, la validità, l'autorizzazione.
L'altro aspetto importante è a livello operazionale, riguardo la scalabilità del protocollo, il tempo di convergenza, la stabilità e le prestazioni.

4.1 Convergenza

I cambiamenti nella rete sono molto comuni, sia a causa di un intervento prestabilito, come ad esempio l'aggiornamento del software di un router, il riavvio di un router, oppure cambiamenti nelle politiche di routing, aggiunta o cancellazione di un prefisso di rete, sia per cause del tutto inaspettate, quali la rottura di un collegamento, un nuovo collegamento introdotto, malfunzionamenti di alcuni router.

Purtroppo i dispositivi di instradamento non riescono a riflettere i cambiamenti immediadamente, per cui ci sarà un periodo di tempo in cui i router dovranno man a mano aggiornare le loro informazioni per riflettere questi cambiamenti, questo periodo di tempo viene chiamato *tempo di convergenza*, quando tutti i router avranno portato a termine i loro aggiornamenti, si dice che la convergenza è stata completata.

La convergenza[10] è un concetto importante per un insieme di router impegnati nell'instradamento dinamico. Un insieme di router dovrebbero

essere convergenti, nel senso che devono aver raccolto tutte le informazioni disponibili sulla topologia della rete uni dagli altri, e queste informazioni raccolte non devono contraddire altre informazioni di qualsiasi altro router nell'insieme, inoltre dovrebbero rispecchiare il reale stato della rete. In altre parole, in una rete convergente tutti i router devono essere d'accordo su ciò che rappresenta la topologia di rete.

Tipicamente i protocolli di instradamento interni si basano su una corretta convergenza per poter funzionare regolarmente, è quello che succede all'interno di ogni AS. Mentre un protocollo di instradamento esterno, qual'è BGP, di solito la convergenza non avviene mai, a causa delle dimensioni troppo grandi di Internet, perchè non si riescono a camunicare velocemente i cambiamenti che avvengono.

Le politiche interne, associate ad un AS, possono risultare ragionevoli sotto il punto di vista della scelta dei percorsi migliori, ma non vi è alcuna garanzia che l'interazione delle politiche locali, anche se ben configurate, di tutti gli AS portino ad una buona convergenza globale. Mentre la maggior parte dei conflitti di politica di routing sono gestibili, con BGP vi è la possibilità che esse potrebbero portare il protocollo a divergere.

A questo punto ci chiediamo se si può garantire che un sistema BGP non diverga. Logicamente la divergenza del BGP potrebbe portare grande instabilità nel sistema globale di instradamento. In generale il problema della convergenza BGP può essere affrontato sia in modo dinamico che statico. Una solouzione dinamica al problema potrebbere essere un meccanismo che reprima o riesca a prevenire, in fase di esecuzione, queste oscillazioni che nascono dai conflitti tra le varie politiche di routing. Uno dei primi meccanismi utilizzati fu il "route flap damping", un meccanismo progettato per limitare selettivamente la propagazione delle informazioni di routing instabili, che però, con l'avanzamento di nuove tecnologie, e di nuovi router in grado di assorbire molto più rapidamente le modifiche alla tabella di routing, è risultato poco efficiente. In primo luogo non elimina l'oscillazione dei percorsi, in secondo luogo non fornisce agli amministratori informazioni sufficienti per identificare l'origine del percorso che ha causato il problema.

Una soluzione statica, invece è quella che si basa sui programmi per l'analisi delle politiche di instradamento, per verificare che non contengano conflitti tra politiche di routing che potrebbero portare divergenze sul protocollo.
Questo è in sostanza l'approccio utilizzando Arbiter Route Project. Questo progetto ha tre componenti. In primo luogo, il Routing Policy Language Specification (RPSL)[11], è un linguaggio di alto livello indipendente dal fornitore per specificare le politiche inter-dominio. In secondo luogo, Internet Route Registries (IRR) sono utilizzati per immagazzinare e distribuire le specifiche RPSL. In terzo luogo, una raccolta di strumenti software, chiama-

to RAToolSet, consente agli amministratori di rete la capacità di manipolare e analizzare le specifiche RPSL che sono state memorizzati nel IRR. Ad esempio, lo strumento RtConfig che genera file di configurazione del router di basso livello in base a specifiche di alto livello descritte con RPSL.

Tra i problemi che si considerano sotto l'aspetto della convergenza ci sono:

- **RAGGIUNGIBILITÀ** Dato un sistema BGP, AS X sarà in grado di importare le rotte originate da AS Y?
- **ASIMMETRIA** Se un sistema BGP permette un routing asimmetrico?
- **RISOLUBILITÀ** Se un dato sistema BGP ha una soluzione?
- **DESTINAZIONE UNICA RISOLUBILE** Se un dato sistema BGP con un'unica destinazione originata da un singolo AS ha una soluzione?
- **UNICITÀ** Se un dato sistema BGP ha una unica soluzione?
- **ROBUSTEZZA** Dato un sistema risolvibile BGP, intende rimanere tale dopo ogni possibile guasto di link X?

Attraverso degli studi effettuati, hanno dimostrato che DESTINAZIONE UNICA RISOLUBILE, ASIMMETRIA e RAGGIUNGIBILITÀ sono NP-completi, nella teoria della complessità, sono problemi difficili da risolvere, mentre RISOLUBILITÀ, UNICITÀ e ROBUSTEZZA sono NP-hard, cioè fanno parte di quella classe di problemi, informalmente definiti come la classe di problemi almeno difficili come i più difficili problemi delle classi di complessità P ed NP.

4.2 Stabilità di routing

Per stabilità di routing intendiamo che un determinato algoritmo dovrà convergere ad una situazione che garantisca appunto la stabilità. In particolare se avvengono errori all'interno della rete che allontanano l'algoritmo dal punto di stabilità, l'algoritmo deve reagire velocemente a questa situazione e riuscire a convergere nuovamente alla stabilità nel minor tempo possibile. Alti livelli di instabilità di rete possono portare alla perdita di pacchetti, aumento della latenza e dei tempi di convergenza. Instabilità di routing, viene informalmente definita come il rapido cambiamento della raggiungibilità delle reti e dell'informazione topologia, ha un certo numero di origini compresi gli

errori di configurazione del router, problemi transitori di collegamento fisico e dati, e bug del software. Instabilità, indicato anche come roure flap, contribuisce in modo significativo alle scarse prestazioni di rete, e diminuisce l'efficienza complessiva dell'infrastruttura di Internet.

Uno studio effettuato sul traffico di routing, divide in tre classi diverse le informazioni di instradamento: l'instabilità d'inoltro, l'oscillazione delle politiche, e aggiornamenti patologici (ridondanti). Questo studio ha dimostrato che la maggior parte delle informazioni di routing, circa il 99%, scambiate all'interno del traffico statunitense è di tipo patologico, e quindi non riflettono i veri cambiamenti della topologia di rete.

I cambiamenti di routing possono causare problemi prestazionali, così come un singolo evento, di cambiamento, può innescare una lunga sequenza di aggiornamenti, dato che ogni speaker BGP avviserà ogni suo vicino del cambiamento avvenuto. Frequenti cambiamenti nella pubblicazione delle rotte verso altri domini, rendono difficoltosa la progettazione del flusso di traffico attraverso un AS. Nei primi studi effettuati si è scoperto un numero allarmante di messaggi di aggiornamento inutili, a causa di scelte progettuali sbagliate. Nonostante il gran numero degli aggiornamenti che si effettuano, una gran parte dei prefissi di destinazione sono percorsi molto stabili.

Un numero relativamente piccolo di prefissi sono responsabili della maggior parte dei messaggi di aggiornamento del BGP. Diversi studi recenti hanno fatto una simile osservazione sui volumi di traffico, che una piccola frazione della destinazione prefissi sono responsabili della maggior parte del traffico Internet. Questo fatto non mostra nulla di incorretto, dato che le destinazioni a cui viene associato la maggior parte del volume del traffico avranno più collegamenti con altri nodi, per garantire una migliore raggiungibilità. Infatti c'è una relazione tra il volume del traffico nella rete e, la stabilita di routing all'interno di un sistema BGP. Basti pensare che un semplice reset di una sessione BGP, risulti in un'esplosione di messaggi di aggiornamento che non riflettono necessariamente i reali cambiamenti avvenuti.

4.3 Topologia

Un altro aspetto importante che riguarda i sistemi di instradamento inter-dominio è capire la topologia della rete da interconnettere. Nell'odierna Internet, la topologia inter-dominio viene determinata dagli accordi commerciali tra i vari fornitori di servizi, per quanto riguarda il traffico di transito. Logicamente un aspetto molto importante legato alla topologia è la crescita della rete, in particolare del numero di prefissi IP indirizzati, causata dal rapido

aumento del numero di host connessi e dal dispiegamento di un'infrastruttura commerciale di Internet.

Un'analisi della topologia della rete è utile sia, per una buona comprensione delle prestazioni delle comunicazione end-to-end, sia perchè potrebbe influenzare la progettazione di futuri protocolli di instradamento e di meccanismi di distribuzione di rotte. Infine una migliore comprensione del sistema di routing è in grado di migliorare la modellazione delle topologie di rete, diminuire i ritardi e le perdite di informazioni.

Dato che Internet è geograficamente distribuita, ed amministrativamente decentrata, è impossibile avere una sua mappa completa, e quindi analizzare la crescita del sistema di instradamento è difficile. Quindi si possono solo effettuare degli studi che simulano l'interconnessione tra domini, e la loro comunicazione.

Conclusioni

In conclusione possiamo dire che il BGP è diventato uno standard a tutti gli effetti, nato per automatizzare il routing inter-dominio, in quanto il numero delle backbone è salito in modo vertiginoso negli ultimi anni e non è più possibile gestirle in modo statico. Il BGP è stato implementato nei primi anni '90, e da allora sono state sviluppate 4 versioni, per rispondere sempre ai più frequenti cambiamenti della rete, e grazie a questi aggiornamenti è riuscito a soddisfare fino ad oggi i requisiti richiesti.
Tutto sommato il BGP si è rilevato come una soluzione piuttosto robusta e scalabile, dato che non c'è un'unica entità amministrativa a gestire il traffico della rete Internet, ma ci sono una serie di accordi fra i vari gestori di rete, per regolare l'instradamento del traffico di transito. Questo sottolinea l'aspetto più importante che BGP evidenzia, cioè la separazione fra meccanismo di funzionamento e politica, per questa ragione ha avuto una così vasto utilizzo.

Un'altro aspetto importante da associare al BGP è il fatto che sia riuscito, grazie a qualche modifica, a supportare fino ad oggi le dimensioni della rete, e quindi a non creare problemi di scalabilità.
Ma come abbiamo descritto in questa tesi, BGP presenta alcune limitazioni. Il problema principale di BGP è rappresentato dalla gestione dei percorsi sovrapposti, che per ora è stato risolto grazie ad alcune funzionalità aggiunte. L'analisi effettuata fin'ora ci permetterà di valutare se questo protocollo sarà in grado di rispondere in modo scalabile, affidabile e sicuro alla crescita costante della rete. In specifico all'aumentare del numero di dispositivi che si aggiungono alla rete. Per ora questo tipo di problema è stato risolto grazie alla strutturazione gerarchica dei dispositivi di rete, che porta ad una crescita "laterale" (molti provider a diversi livelli, e il numero costante di livelli) anziché "verticale", ma non siamo sicuri che queste tecniche aiutano a risolvere il problema della scalabiltà in modo definitivo.
Per avere un quadro completo sul BGP, per capire meglio il suo funzionamento si possono analizzare diverse implementazioni:

- OpenBGPD
- Quagga
- Xorp
- Zebra
- BIRD

Un altro punto a sfavore del BGP, è dovuto al fatto che le politiche di routing devono essere implementate manualmente in ogni router BGP. Questo aspetto unito alla mancanza di sofisticati strumenti per l'analisi dell'instradamento, e a strumenti di debug diminuiscono il livello di stabilità della rete.

Non c'è alcun motivo per ritenere che il modello di crescita nella topologia inter-domain cambierà significativamente nel prossimo futuro. Tuttavia, un'infrastruttura sempre più commerciale e competitiva è probabile che stimolano lo sviluppo di analisi di routing automatizzate e di strumenti di ingegneria, con conseguente miglioramento della stabilità di routing.

BGP non è l'unico protocollo per l'instradamento inter-dominio, sono stati implementati anche altri protolli, quali Inter Domain Routing Protocol (IDRP)[14], che migliora la memorizzazione delle tabelle, è stato dimostrato che in determinate ipotesi piuttosto generali la complessità di conservazione del IDRP è ottimale, o molto vicina al valore ottimale. Ma anche questo tipo di protocollo non è una soluzione molto efficace a causa del dispendio di calcolo nelle fasi crittografiche e in quelle di controllo.

Bibliografia

[1] Y. Rekhter, T. Li, S. Hares. *A Border Gateway Protocol 4 (BGP-4).* RFC 4271 January 2006.

[2] A.S. Tanenbaum. *Reti di calcolatori.* 2005 (quarta edizione) Pearson Education.

[3] Larry L. Peterson, Bruce S. Davie. *Reti di calcolatori.* 2004 (terza edizione) Apogeo pp. 266-275.

[4] J. Hawkinson BBN Planet, T. Bates MCI. *Guidelines for creation, selection, and registration of an Autonomous System.* RFC 1930 Marzo 1996.

[5] James F. Kurose, Keith W. Ross. *Internet e Reti di Calcolatori.* 2003 (seconda edizione) Mc. Graw Hill pp 329-341.

[6] Larry L. Peterson, Bruce S. Davie. *Reti di calcolatori.* 2004 (terza edizione) Apogeo pp 262, pp 277.

[7] C. Metz. *Interconnecting ISP Networks*, IEEE Internet Computing. Marzo 2001 pp. 74-80.

[8] S. Kent, C. Lynn, K. Seo. *Secure Border Gateway Protocol* IEEE JOURNAL ON SELECTED AREA IN COMMUNICATIONS, VOL.18, NO. 4. Aprile 2000.

[9] J. Rexford, J. Wang, Z. Xiao, Y. Zhang. *BGP Routing Stability of Popular Destinations.*

[10] T.G. Griffin, G.Wilfong. *An Analysis of BGP Convergence Properies.* 1999.

[11] C. Alaettinoglu, T. Bates, E. Gerich, D. Karrenbcrg, D. Meyer, M. Terpstra, and C. Villamizar. *Routing Policy Specification Language (RPSL).* RFC 2280, 1998.

[12] L. Subramanian, V. Roth, I. Stoica, S. Shenker, R.H. Katz. *Listen and Whisper: Security Mechanism for BGP* 2003.

[13] D. Lee, M. Yannakakis. *Principles and methods of testing finite state machines-a survey.* Proceedings of the IEEE. pp 1090 - 1123, Agosto 1996.

[14] *Protocol for Exchange of Inter-domain Routeing Information among Intermediate Systems to Support Forwarding of ISO 8473 PDUs* IEC/ JTC1/SC 6 CD10747.

[15] V. Gill, J. Heasley, D. Meyer, P. Savola, C. Pignataro. *The Generalized TTL Security Mechanism (GTSM).* RFC 5082 Ottobre 2007.

[16] T. Wan, E. Kranakis, P.C. van Oorschot. *Pretty Secure BGP (psBGP).*

[17] A. Heffernan. *Protection of BGP Sessions via the TCP MD5 Signature Option.* RFC 2385 Agosto 1998.